

DARPA On-Site Contractor Security Guidance

I. General

- a. Contractor Performance. In performance of this Contract the following security services and procedures are incorporated as an attachment to the DD Form 254. The Contractor will conform to the requirements of DoD 5220.22-M, Department of Defense National Industrial Security Program Operating Manual (NISPOM). Additionally, when visiting or working at DARPA facilities the Contractor will comply with the DARPA Security Manual relative to DARPA security policies and procedures as they apply to the protection of classified and sensitive but unclassified information. If the contractor establishes a cleared facility or Defense Security Service approved off-site location in support of this contract the security provisions of the NISPOM alone will apply to that facility.
- b. Security Supervision. DARPA will exercise security oversight over all contractors visiting or working at DARPA. The contractor will identify, in writing, to the Director, Security and Intelligence Directorate (SID), an on-site management Point of Contact (POC) that will interface with the DARPA SID for security matters. Additionally, the contractor shall provide SID, in writing, the name, address, telephone number, and email address of the Company's cognizant Facility Security Officer (FSO). The contractor shall ensure that these names and addresses are kept current.
- c. Basic Requirement. Personnel who are issued either an On-Site or Off-Site DARPA identification badge and/or who are granted access to DARPA facilities and/or to the DARPA Management Support System (DMSS) must have, at a minimum, a current SECRET clearance under the sponsorship of the employing contractor. The contractor shall establish a system to immediately notify the Director, SID, and immediately deny access to DARPA facilities and the DMSS, when a contractor employee's clearance is withdrawn or administratively downgraded for any reason.
- d. Security Classification Guide (SCG). The contractor shall ensure that the appropriate SCG is used to determine classification requirements for DARPA information and material. Questions regarding classification may be directed to the Director, SID.

II. Handling Classified Material or Information

- a. Control and Safeguarding. Contractor personnel working at DARPA or traveling to support DARPA efforts are responsible for the control and safeguarding of all classified and sensitive material in their possession. All contractor personnel will be briefed by their company on their individual responsibilities to safeguard classified

material. In addition, all contractor personnel authorized a DARPA badge are required to attend the DARPA Security Orientation Briefing prior to badge issuance. The Security Orientation Briefings are routinely scheduled twice weekly. Contact the DARPA badge office for further information. In the event of possible or actual loss or compromise of classified material, the on-site Contractor point of contact (POC) at DARPA will immediately report the incident to DARPA SID. This does not negate the need for the POC to promptly report the incident to the supported DARPA Technical Office management representative. A DARPA SID representative will conduct an inquiry of the incident and provide a report to the FSO and the Cognizant Field Office of the DSS if the event involves Contractor personnel. The contractor will promptly correct any deficient security conditions identified by the DARPA SID.

b. Storage.

1. Classified material may only be stored in containers authorized by and registered in the DARPA Classified Document Registry (CDR). Containers are assigned to a Primary Custodian and, where necessary, alternate custodians are appointed. On-site contractor personnel may act as custodians. Custodians must be properly listed on the Standard Form 700 and must be properly registered with the CDR. The contractor will establish a system to assure that the CDR is promptly notified when their personnel no longer need access to a container and that all personnel to whom classified documents have been issued or that were custodians process out through the CDR and turn in all classified material to the CDR prior to their departure. The custodian will notify the CDR when a container is to be relocated or turned in or when there is a change in personnel that are authorized access to the container.

2. Only DARPA SID approved areas are authorized for the open storage and processing of classified material. All other areas within DARPA facilities are governed by proper In-Use-Controls. The term "In-Use-Controls" is defined as: When classified material is removed from the container, appropriately cleared personnel with the requisite need-to-know must exercise physical control of the material at all times. Additionally, other controls such as closing the office blinds, positioning computer monitors, and/or shutting the office doors shall be utilized to preclude unauthorized disclosure of classified material/information.

c. Transmission of Classified Material.

1. All classified (collateral) material transmitted by mail or courier for use by Contractor or DARPA Staff will be addressed to:

Defense Advanced Research Projects Agency
ATTN: CDR
3701 N. Fairfax Drive
Arlington, VA 22203

The inner envelope will be addressed to the attention of the person for whom the material is intended.

2. All classified collateral material, regardless of classification, that is hand carried to DARPA by contractor personnel must be delivered to the CDR for processing. Special arrangements must be made with the Director, SID, for the hand-carrying of Sensitive Compartmented Information (SCI) or Special Access Program (SAP) material,
3. All DARPA classified material that is transmitted from DARPA facilities, regardless of method, will be processed by the CDR.

III. Information Systems (IS) Security.

- a. Contractors using DARPA information systems, networks or computer resources will comply with the provisions of applicable DoD and DARPA Directives and Instructions governing their use.
- b. Access to DARPA information systems is limited to Government Staff and approved contractor employees who have been issued the requisite system privileges. Under no circumstance shall a visiting or assigned contractor employee and/or representative obtain access to, connect to, or otherwise interface with any DARPA information system (classified or unclassified) without prior written approval from the DARPA Information System Security Officer. This includes the attaching of unapproved laptops and other hardware peripherals to the DARPA Management Support System (DMSS) and stand-alone systems.
- c. The loss, theft, destruction, or suspected compromise of any DARPA computer or computer system will be immediately reported to the Director, SID. The contractor shall establish a system to assure that any DARPA issued or owned electronic equipment (e.g. telephone, computer, etc.,) is properly turned in to proper DARPA channels prior to the departure of their personnel.

IV. Physical Security/Access Controls Procedures.

- a. DARPA will provide appropriate response to emergencies occurring within DARPA facilities. The Contractor will comply with all emergency rules and procedures established for DARPA.
- b. All personnel assigned to or visiting DARPA facilities are subject to random inspections of their vehicles, personal items in their possession, and of their persons. Consent to these inspections is considered granted when personnel accept either a badge or a vehicle-parking pass that permits access into DARPA controlled facilities.
- c. The DARPA SID Badge Office will issue either an "On-Site" or "Off-Site" Contractor identification badge to contractor personnel who are sponsored and

authorized by their respective DARPA Office. Prior to badge issuance, a current Visit Authorization Letter (VAL) must be on file, a DARPA Form 37, Badge Request, must be completed, and the personnel who is being issued the badge must have attended the Security Orientation Briefing. The preparation and submission of the necessary forms for obtaining a badge is the responsibility of the contractor.

d. Contractor personnel not physically located/assigned to DARPA but who require frequent access to DARPA facilities in the performance of their contract may be eligible for an Off-site Contractor identification badge. The procedures for obtaining this badge are the same as described above.

e. The respective DARPA Offices may at their discretion authorize the issuance of the On-Site identification badge for a period not to exceed the length of the basic contract or option period. The Director, SID, in consonance with the sponsoring DARPA office, will determine the expiration date for the Off-Site badge. Identification badges are the property of the U.S. Government and will be worn and used for official business only. Identification badges must be worn above the waist in plain sight at all times within DARPA facilities. Lost or misplaced badges must be immediately reported to SID (within one working day). Additionally, the FSO and the person to whom the badge is issued shall promptly report a name change, clearance level change, or transfer within DARPA offices, to the DARPA badge office. The contractor shall establish a system to assure that the DARPA badge office is promptly notified of such changes or when a person issued a DARPA badge is terminating employment with the company or is transferring within the company and will no longer need access to DARPA facilities. The need for transferring personnel to retain a DARPA badge shall be determined by the Director, SID. The contractor shall be responsible for assuring that the badges for such personnel are turned in to the DARPA badge office prior to their departure.

f. All classified visits by contractor personnel, On-Site, Off-Site, or other, require the submission of a VAL in accordance with the NISPOM. Visitors that are not issued On-Site or Off-Site badges must be processed through the DARPA Visitor Control Center and present a valid form of identification prior to each admittance to DARPA controlled areas. Such personnel shall be issued a DARPA visitor badge. The contractor VALs shall be mailed, or faxed to:

Defense Advanced Research Projects Agency
Attn: Visitor Control Center
3701 N. Fairfax Drive
Arlington, VA 22203

Phone : (703)528-3902 Fax : (703)528-3655

g. The contractor shall establish a system to ensure prior notification to SID when visits to DARPA facilities by Foreign Nationals, to include those employed by the contractor, are desired. The visit by a foreign national employee may require the

possession of an Export Control License by the contractor and proof of such license may be required before the visit is approved. The contractor shall ensure compliance with DARPA escort and badge requirements for foreign nationals.

V. Security Compliance Inspections.

DARPA SID personnel will conduct periodic inspections of DARPA facilities and off-site contractor facilities that are using DARPA computer systems. The contractor shall ensure that all contract personnel fully cooperate with DARPA SID representatives during these inspections. A report of the inspection will be forwarded, through appropriate contract channels, to the contractor and the appropriate contractor's COR. The contractor will take prompt action to correct identified deficiencies.

VI. Reports.

As required by the NISPOM, contractors are required to report events that impact their facility clearance (FCL), an employee's personnel clearance (PCL), the ability to properly safeguard classified information, or an indication that classified information has been lost or compromised. The Contractor will ensure that when such events impact, or potentially impact DARPA personnel, operations, or information, they are also promptly reported to the SID. Examples of such events include, but are not limited to the following:

- a. The denial, suspension or revocation of a security clearance of any assigned person, or the suspension, revocation or denial of a FCL connected to a DARPA contract.
- b. Any adverse information which would cast doubt on an assigned employee's continued suitability for continued access to classified information, material, or facilities;
- c. Any instance of loss or compromise, or suspected loss or compromise, of classified information;
- d. Actual, probable or possible espionage, sabotage, or subversive information;
- e. The loss, theft, or destruction of any DARPA issued or owned equipment or material.

VII. Escort Policy

The contractor shall establish a system to ensure compliance with DARPA's escort policy.

VIII. Special Considerations for DARPA Enclave Facilities.

Any contractor occupied space within DARPA facilities will be used strictly for official business in support of DARPA efforts.

IX. Items Prohibited Within DARPA Facilities.

a. Dangerous weapons, instruments or devices. This includes, but is not limited to, the following:

- Rifles, automatic rifles, machine guns, sub-machine guns, pistols, machine pistols, flare pistols, starter pistols, shotguns, compressed gas, air or spring fired pellet or “BB” guns, sling shots, blow guns, or any other device which uses gun powder, compressed gas or air, or spring tension to forcefully eject a projectile or other device which may injure someone;
- Daggers, switch blades, bow and arrows, spear guns, Hawaiian slings, power heads, fishing knives, scuba knives, or any knife with a blade longer than 2 ½ inches (Knives used for authorized construction and or repair efforts are excluded from this prohibition);
- Martial arts devices (throwing stars, nunchuks), stun guns, Tasers, brass knuckles, billy clubs, night sticks, pipe, bars, or mallets, or other similar devices capable of being used as a weapon;
- Poison, acids or caustic chemicals;
- Any other item that may be used to inflict serious injury or death to another person or temporarily blind or disable an individual and which have not been specifically authorized by proper authority.

b. Explosive article or compound. This includes but is not limited to: ammunition for any of the small arms weapons mentioned as a dangerous weapon, including “blank” ammunition, gunpowder, Molotov cocktails, pipe bombs, grenades, pyrotechnics, fireworks or any other compound or article which might violently react and cause injury not specifically authorized by proper authority.

X. Contractor Check-Out Procedures

The contractor shall establish a system to ensure a "check-out" procedure for all contract employees who have been issued a DARPA on-site or off-site badge. The system shall ensure that all badges, keys, classified documents, equipment, communications security equipment (COMSEC)/material, etc., are turned in to proper DARPA channels prior to the employee's departure or transfer.

XI. Investigations and Inquiries

DARPA SID personnel may be required to conduct various investigations or inquiries where contractor employees are or may be involved. The contractor shall ensure that all contract personnel fully cooperate with DARPA SID representatives during these efforts. Information and documents requested by DARPA SID representatives will be promptly

provided and shall be provided in compliance with Federal and State law and regulation. A report of the inquiry or investigation will be forwarded, through appropriate contract channels, to the Contractor's employing facility and COR. The contractor will take prompt action to correct identified deficiencies and will provide a written report of the actions taken through contract channels to the Director, SID.

XII. Clearance for Public Release

All appropriate information resulting or derived from DARPA funded efforts that is intended for public release must be submitted for DARPA approval in accordance with DARPA Instruction 65, Clearance of DARPA Information for Public Release.

XIII. Preparation of DD Forms 254

The contractor shall ensure that DARPA security requirements, to include the appropriate SCG, are flowed down to their subcontractors who are involved in DARPA efforts. A copy of all DD Forms 254 issued to subcontractors performing DARPA work will be provided to the Director, SID.